## Skyhigh Threat Protection & Activity Monitoring

The following Omnibar facets can be used on either the Threat Protection or Activity Monitoring pages.

|  |  |  |
| --- | --- | --- |
| Search Term | Description | Available Options |
| Action Name | The name of the detected activity. You can use this Omnibar facet to filter on specific activities that you wish to investigate. You may need to learn more about how many users are engaging in a specific activity or investigate threats that are calculated based on your selected activity. | Select one or more available activities. |
| Anomaly Category | The organizational categories used to sort detected anomalies. You can use this Omnibar facet to investigate all anomalies that are sorted into one of the three categories. Filtering by category can help with anomaly resolution; if you deal with one category at a time the list may be more easily managed.  | Administration Anomalies |
| Data Anomalies |
| Access Anomalies |
| Anomaly Duration | The length of time that the anomaly took place. You can use this Omnibar facet to filter your anomaly list based on the longest running anomalies. Anomalies that have been measured over longer timelines are more likely to indicate valid threats. | Hourly |
| Daily |
| Weekly |
| Monthly |
| Anomaly Name | The name of the specific anomaly. You can use this Omnibar facet to filter on a particular anomaly in order to investigate security events; if you have an account breach you can check into any unusual file transfers that occurred during the breach. | Only anomalies that have been detected for the active CSP will be available for selection. |
| At this time, users can only filter results by name for Superhuman, Brute Force Login, and Large Report Download anomalies. If you wish to filter based on anomalies in the Data Anomalies category, you should use the Anomaly Category filter instead.  |
| Anomaly Threshold | This Omnibar facet is reserved for internal functionality. | N/A |

|  |  |  |
| --- | --- | --- |
| Search Term | Description | Available Options |
| Category | The category of the detected activity. You can use this Omnibar facet to filter on specific activity types. Filtering by category can help with activity monitoring; if you deal with one category at a time the list may be more easy to manage.  | <This appears to be the same list as activity name. What's the difference?> |
| Valli - e.g download category refers to several download activity names like - Download File, Download Folder, so here you are searching at a category level. |
| Client Browser | The web browser used to create the activity or anomaly. You can use this Omnibar facet to gain additional insight into how your users are interacting with your cloud services and learn about potential anomaly patterns that may influence your device management rules. For example, if the majority of your access anomalies are occurring through an insecure browser, you may wish to block users from connecting to the cloud service using that browser. | Select one or more detected browsers. |
| Client OS | The computer operating system used to create the activity or anomaly. You can use this Omnibar facet to gain additional insight into how your users are interacting with your cloud services and learn about potential anomaly patterns that may influence your device management rules. For example, if the majority of your access anomalies are occurring through an insecure OS, you may wish to block users from connecting to the cloud service using that OS. | Select one or more detected operating systems. |
| Collaboration Group | The domain of the user's email address. For example, if you detect activity from users with email address ending in samplecompany.com, competetorcompany.com and freeemail.com, there will be three detected collaboration groups. You can use this Omnibar facet on the Collaboration View to filter collaborations to specific domains. | Select one or more of the detected collaboration groups for the CSP. |

|  |  |  |
| --- | --- | --- |
| Search Term | Description | Available Options |
| Country | The country where the activity or anomaly occurred. You can use this Omnibar facet to understand anomaly and threat patterns occurring in different countries. If excessive anomalies occur in a specific country you can adjust your access and DLP policies surrounding access in that country. | Select one or more detected countries. <Is there an abbreviation to country list I can use?> |
| Device | The device used to trigger the activity or anomaly. You can use this Omnibar facet to gain additional insight into how your users are interacting with your cloud services and learn about potential anomaly patterns that may influence your device management rules. For example, if the majority of your access anomalies are occurring through an insecure device, you may wish to block users from connecting to the cloud service using that device. | Select one or more of the detected devices. |
| Logical Operators | Use these operators to create compound Omnibar searches. You can use this Omnibar facet link multiple facets together in a single search string. For example, you can search for all anomalies in the Data Anomalies group made to Box from China. | And |
| Or |
| ( |
| ) |
| Notes | This Omnibar facet is reserved for future functionality. | N/A |
| Profile | The profile of the user who triggered the activity or anomaly. Profile information is provided through your Salesforce or Active Directory integration. You can use this Omnibar facet to discover more about the activities of specific types of users. For example, if you've established the profile of "Sales Team" you can filter your results based on that profile. | Select one or more detected profiles. |

|  |  |  |
| --- | --- | --- |
| Search Term | Description | Available Options |
| Role | The role of the user who triggered the activity or anomaly. Role information is provided through your Salesforce or Active Directory integration. You can use this Omnibar facet to discover more about the activities of specific types of users. For example, if you've established the role of "Accounting" you can filter your results based on that role. | Select one or more detected role. |
| Service Name | The CSP where the activity or anomaly occurred. You can use this Omnibar facet to learn more about the activities occurring in a specific service in order to better design DLP policies for this service.  | Only the currently selected service can be used in this facet. However, Skyhigh for O365 customers can use this facet to separate SharePoint, AzureAD or OneDrive results. |
| Severity | The severity of the anomaly, as determined by how much the anomaly exceeds its threshold. You can use this Omnibar facet to manage your investigation workflow; filtering based on severity level allows your investigators to focus on the highest priority anomalies or threats first. | High |
| Medium |
| Low |
| Status | This Omnibar facet is reserved for internal functionality. | N/A |
| Threat Category | The organizational categories used to sort detected threats. You can use this Omnibar facet to investigate all threats that are sorted into one of the three categories. Filtering by category can help with threat resolution; if you deal with one category at a time the list may be more easy to manage.  | Compromised Accounts |
| Privileged Access |
| Threat Name | The name of the specific threat. You can use this Omnibar facet to filter on specific threats that you wish to investigate. You may need to learn more about how often this threat occurs or which sorts of users trigger this threat. | Only threats that have been detected for the active CSP will be available for selection.  |

# About the Omnibar

Table of contents No headers

Appearing across many aspects of the Skyhigh Networks service, the Omnibar serves as a comprehensive search and filtering tool.

From the Omnibar, you can search for information across multiple sections of the product and filter the results based on a contextual menu that’s appropriate for your selections.

Specifically, you can search for services, users, categories, and more without having to move to a different screen.

The Omnibar is available in the Usage Analytics and Incident Management sections of Skyhigh.

Use the Omnibar to search in the following ways:

* Type into the Omnibar directly. Predictive search suggests available search terms before you finish your query.
* To use the Date Picker to select a date range for your search, relative or explicit, click the **calendar** icon.
* To add a filter to your search, click the **funnel** icon and select filters from the **Add a Filter** dialog.
* To create a saved view, click the **star** icon.
* To use a saved view or default perspective, click the **down arrow** icon.
* As you add components to build your search, they are displayed as "pills" in the Omnibar.
* To remove search component "pills", click the **x** next to the component.
* Press **Enter**, or click the **magnifying glass** icon to start your search.